



# Diebold Anti Skimming and Phishing Solution

ISSUE 5

SEPTEMBER 14, 2011

## About

### TouchPoint

TouchPoint (Pvt.) Limited is the sole distributor of Diebold's ATMs within Pakistan. We offer the best secured services solution to our customers that completely fulfill their needs.

Our product line includes Opteva ATMs, advance teller automation & technology, safety products. TouchPoint (Pvt.) Limited has made significant steps forward with prestigious names to its customer base. We strive towards providing innovative out of the box, personalized services which always have a novel element.

We intend to transform the 'Six Star Services Vision' into reality. For more information, please visit

[www.touchpoint.pk](http://www.touchpoint.pk)

## About



Diebold, Incorporation is a global leader in providing integrated self-service delivery and security systems and services. Diebold employs more than 16,000 associates with representation in nearly 90 countries worldwide.

Diebold is publicly traded on the New York Stock Exchange under the symbol 'DBD.' For more information, please visit

[www.diebold.com](http://www.diebold.com)

## Pakistan's 1st Skimming Case

Pakistan's first ATM skimming case was reported this year against local university students who used automated teller machine (ATM) skimming scam and allegedly prepared a skimmer to elicit data from ATM cards and deprived cardholders of millions of rupees.

The five accused fraudulently accessed the information systems of Bank / Visa International / Master Cards data and subsequently made fake transactions on the same card accounts by using the counterfeit credit cards incurring Bank Al-Falah a loss of over Rs. one million.

FIA investigation reveals that skimmer is a small electronic device that the criminal attaches to a credit card terminal or ATM. Every time a card is inserted or swiped through the machine the skimmer gathers user's information and it may be attached to a device that logs keystrokes to collect the personal identity numbers (PINs) of people who use the terminal.

### Diebold Anti Skimming and Phishing Solution

Diebold's skimming and phishing protection packages offer the latest generation of proven technologies and leverage the most innovative anti-skimming expertise in the industry. Five levels of security are available to help guard against the most sophisticated card-skimming attacks.

#### Level 1 Protection

Minimum level of protection for ATMs located in the branch or locations where risk is minimal for skimming. Multi-layered security features are integrated into the card reader and feature a unique bezel design that helps deter against skimmer attachment. Lead-through indicator flashing LEDs can also alert consumers if skimming device placed on the front of card reader.



Diebold's PIN pad shield, along with surveillance technology helps prevent the capture of PIN.

#### Level 2 Protection

Skimming-detection technology detects a skimmer and generates an automatic alert that a fraudulent device has been added to the card-reader bezel. This alert can be directed either to the branch alarm system or to the ATM network monitoring system whenever a skimming attempt is detected.

#### Level 3 Protection

Additional level of protection against skimming, leveraging our self-service security expertise with TMD Security's jamming, anti-skimming technology. TMD solution for dip card readers does not permit card reader and the skimmer to read the card, so a transaction cannot be started—taking the terminal out of service until the threat has been removed, helping to protect cardholder information.

#### Level 4 Protection

Higher level of protection combining TMD Security's detection and jamming for Opteva, multi-vendor and legacy terminals in locations where risk is high for skimming.

#### Level 5 Protection

Offers customized response plans featuring e-mail alerts and text messages from the Monitoring Center, voice notification and follow-up, as well as Diebold service technicians to inspect ATM and video verification to confirm the presence of a skimming device.

#### Best Practices to Mitigate

#### Skimming/Phishing Frauds

- Build awareness among consumers, branch personnel and ATM service teams. Visual cues such as tape residue near or on a card reader may indicate former presence of a skimming device.
- Video surveillance and monitoring are effective methods for detecting card skimmers and other fraudulent devices such as PIN overlays and mini-cameras.
- Implement multiple layers of security to help deter and detect fraudulent attempts to provide the best approach to anti-skimming.
- Alert systems monitor the routine patterns of withdrawals and notify operators or financial institutions in the event of suspicious activity.